WHAT IS CLAIMED IS:

1. A method comprising:

providing a host computer system having at least one network interface interfaced with a computer network;

operating the host computer system in a multi-user mode;

detecting an intrusion event using a system daemon; and

in response to detecting the intrusion event, isolating the at least one network interface from the computer network and taking the host computer system down to a single user state so that access to the host computer system is limited to physical access at the host computer system.

2. The method of claim 1 wherein the system daemon comprises a JTRIP system daemon.

3. The method of claim 1 wherein said isolating the at least one network interface from the computer network comprises issuing an IFCONFIG down command to the at least one network interface.

4. The method of claim 1 wherein said taking the host computer system down to the single user state comprises issuing an INIT1 command to an operating system of the host computer system.

5. The method of claim 1 further comprising:

reading, by the system daemon, a configuration file that indicates at least one file in a file system of the host computer system to be monitored for intrusion.

6. The method of claim 5 wherein the configuration file comprises a first directive type that indicates a directory whose members are to be monitored for intrusion, a second directive type that indicates a file to be monitored for intrusion, and a third directive type that indicates another configuration file to be monitored for intrusion.

7. The method of claim 1 further comprising:

computing a data verification signature for a monitored file in a file system of the host computer system; and

comparing the data verification signature to a valid data verification signature for the monitored file;

wherein said detecting the intrusion event comprises detecting that the data verification signature differs from the valid data verification signature.

8. The method of claim 7 wherein the valid data verification signature comprises a Message Digest 5 (MD5) signature.

9. The method of claim 7 further comprising:

reading the valid data verification signature for the monitored file from a database that is located on a second computer system isolated physically and programmatically from the host computer system.

10. The method of claim 9 further comprising:

writing a log of the intrusion event to a log database that is not located on the host computer system or second computer system.

11. The method of claim 1 wherein said detecting the intrusion event comprises detecting an incorrect permission associated with a file in a file system of the host computer system.

12. The method of claim 1 wherein said detecting the intrusion event comprises detecting an incorrect ownership associated with a file in a file system of the host computer system.

13. The method of claim 1 wherein said detecting the intrusion event comprises detecting that a file no longer exists in a file system of the host computer system.

14. A method comprising:

providing a host computer system having at least one network interface interfaced with a computer network;

operating the host computer system in a multi-user mode;

executing a JTRIP system daemon on the host computer system;

reading, by the JTRIP system daemon, a configuration file that indicates at least one file in a file system of the host computer system to be monitored for intrusion, wherein the configuration file comprises a first directive type that indicates a directory whose members are to be monitored for intrusion, a second directive type that indicates a file to be monitored for intrusion, and a third directive type that indicates another configuration file to be monitored for intrusion;

reading a valid MD5 signature for a monitored file from a database that is located on a second computer system isolated physically and programmatically from the host computer system;

detecting an intrusion event using the JTRIP system daemon by detecting that an MD5 signature of the monitored file differs from the valid MD5 signature; and

in response to detecting the intrusion event:

issuing an IFCONFIG down command to the at least one network interface to isolate the at least one network interface from the computer network;

issuing an INIT1 command to an operating system of the host computer system to take the host computer system down to a single user state; and

writing a log of the intrusion event to a log database that is not located on the second computer system.

15. A system comprising:

a host computer system having at least one network interface interfaced with a computer network, the host computer system to:

operate in a multi-user mode;

detect an intrusion event using a system daemon; and

in response to detecting the intrusion event, isolate the at least one network interface from the computer network and take the host computer system down to a single user state so that access to the host computer system is limited to physical access at the host computer system.

16. The system of claim 15 wherein the system daemon comprises a JTRIP system daemon.

17. The system of claim 15 wherein the host computer system is to isolate the at least one network interface from the computer network by issuing an IFCONFIG down command to the at least one network interface.

18. The system of claim 15 wherein the host computer system is taken down to the single user state by issuing an INIT1 command to an operating system of the host computer system.

19. The system of claim 15 wherein the host computer system is further to read, by the system daemon, a configuration file that indicates at least one file in a file system of the host computer system to be monitored for intrusion.

20. The system of claim 19 wherein the configuration file comprises a first directive type that indicates a directory whose members are to be monitored for intrusion, a second directive type that indicates a file to be monitored for intrusion, and a third directive type that indicates another configuration file to be monitored for intrusion.

21. The system of claim 15 wherein the host computer system is further to:

compute a data verification signature for a monitored file in a file system of the host computer system; and

compare the data verification signature to a valid data verification signature for the monitored file;

wherein the intrusion event is detected by detecting that the data verification signature differs from the valid data verification signature.

22. The system of claim 21 wherein the valid data verification signature comprises a Message Digest 5 (MD5) signature.

23. The system of claim 21 further comprising:

a second computer system isolated physically and programmatically from the host computer system;

wherein the host computer system is to read the valid data verification signature for the monitored file from a database that is located on the second computer system.

24. The system of claim 23 further comprising:

a log database not located on the host computer system or the second computer system;

wherein the host computer system is further to write a log of the intrusion event to the log database.

25. The system of claim 15 wherein the intrusion event comprises an incorrect permission associated with a file in a file system of the host computer system.

26. The system of claim 15 wherein the intrusion event comprises an incorrect ownership associated with a file in a file system of the host computer system.

27. The system of claim 15 wherein the intrusion event comprises a file no longer existing in a file system of the host computer system.